ABSTRACT OF THE DISCLOSURE

An inter-equipment authentication and key delivery scheme, system, and equipment is provided which is capable of making authentication of an IC card ID signature, by comparison of a decrypted ICCID with another ICCID reproduced by dividing transmitted data. The inter-equipment authentication and key delivery scheme, system, and equipment can be used, for example, when an automobile passes by roadside equipment at a tollbooth, and the roadside equipment transmits a random digit (RND) generated therein as challenge data to an IC card via onboard equipment, and the IC card transmits back to the roadside equipment the random digit after encrypting it with a secret key Kicc. The IC card also transmits its ID (ICCID) and a certificate of individual IC card key CERT-Kicc together with the random digit . The roadside equipment divides the transmitted data into a response data E(Kicc, RND), the ICCID, and the certificate of individual IC card key CERT-Kicc. The roadside equipment 130 reproduces the Kicc and the ICCID by decrypting (DEC) the certificate of individual IC card key CERT-Kicc using a validation key PC.